FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1639656-000

Total Deleted Page(s) = 204
Page 8 ~ Duplicate - Serial 61;
Page 9 ~ Duplicate - Serial 61;
Page 10 ~ Duplicate - Serial 61;
Page 11 ~ Duplicate - Serial 61;
Page 12 ~ Duplicate - Serial 61;
Page 13 ~ Duplicate - Serial 60;
Page 14 ~ Duplicate - Serial 60;
Page 15 ~ Duplicate - Serial 60;
Page 16 ~ Duplicate - Serial 60;
Page 17 ~ Duplicate - Serial 60;
Page 18 ~ Duplicate - Serial 60;
Page 19 ~ Duplicate - Serial 60;
Page 20 ~ Duplicate - Serial 60;
Page 21 ~ Duplicate - Serial 60;
Page 22 ~ Duplicate - Serial 60;
Page 23 ~ Duplicate - Serial 60;
Page 24 ~ Duplicate - Serial 60;
Page 25 ~ Duplicate - Serial 60;
Page 26 ~ Duplicate - Serial 60;
Page 27 ~ Duplicate - Serial 60;
Page 28 ~ Duplicate - Serial 60;
Page 29 ~ Referral/Direct;
Page 30 ~ Referral/Direct;
Page 31 ~ Referral/Direct;
Page 32 ~ Referral/Direct;
Page 33 ~ Referral/Direct;
Page 34 ~ Referral/Direct;
Page 35 ~ Referral/Direct;
Page 36 ~ Referral/Direct;
Page 37 ~ Referral/Direct;
Page 38 ~ Referral/Direct;
Page 39 ~ Referral/Direct;
Page 40 ~ Referral/Direct;
Page 41 ~ Referral/Direct;
Page 42 ~ Referral/Direct;
Page 43 ~ Referral/Direct;
Page 44 ~ Referral/Direct;
Page 45 ~ Referral/Direct;
Page 46 ~ Referral/Direct;
Page 47 ~ Referral/Direct;
Page 48 ~ Referral/Direct;
Page 49 ~ Referral/Direct;
Page 50 ~ Referral/Direct;
Page 51 ~ Referral/Direct;
Page 52 ~ Referral/Direct;
Page 53 ~ Referral/Direct;
Page 54 ~ Referral/Direct;
Page 55 ~ Referral/Direct;
Page 56 ~ Referral/Direct;
Page 57 ~ Referral/Direct;
Page 58 ~ Referral/Direct;
Page 59 ~ Referral/Direct;
Page 60 ~ Referral/Direct;
Page 61 ~ Referral/Direct;
Page 62 ~ Referral/Direct;
Page 63 ~ Referral/Direct;
Page 64 ~ Referral/Direct;
Page 65 ~ Referral/Direct;
Page 66 ~ Referral/Direct;
Page 67 ~ Referral/Direct;
Page 68 ~ Referral/Direct;
Page 69 ~ Referral/Direct;
Page 70 ~ Referral/Direct;
Page 71 ~ Referral/Direct;
Page 72 ~ Referral/Direct;
Page 73 ~ Referral/Direct;
Page 74 ~ Referral/Direct;

Page 75 ~ Referral/Direct;
Page 76 ~ Referral/Direct;
Page 77 ~ Referral/Direct;
Page 78 ~ Referral/Direct;
Page 79 ~ Referral/Direct;
Page 93 ~ b5; b7E;
Page 94 ~ b5; b7E;
Page 95 ~ b5; b7E;
Page 96 ~ b5; b7E;
Page 97 ~ b5; b7E;
Page 119 ~ Referral/Direct;
Page 120 ~ Referral/Direct;
Page 121 ~ Referral/Direct;
Page 122 ~ Referral/Direct;
Page 123 ~ Referral/Direct;
Page 124 ~ Referral/Direct;
Page 125 ~ Referral/Direct;
Page 126 ~ Referral/Direct;
Page 127 ~ Duplicate - Serial 64;
Page 128 ~ Duplicate - Serial 64;
Page 129 ~ Duplicate - Serial 64;
Page 130 ~ Duplicate - Serial 64;
Page 131 ~ Duplicate - Serial 64;
Page 132 ~ Duplicate - Serial 64;
Page 133 ~ Duplicate - Serial 64;
Page 134 ~ Duplicate - Serial 64;
Page 135 ~ Duplicate - Serial 64;
Page 136 ~ Duplicate - Serial 64;
Page 137 ~ Duplicate - Serial 64;
Page 138 ~ Duplicate - Serial 64;
Page 139 ~ Duplicate - Serial 64;
Page 140 ~ Duplicate - Serial 64;
Page 141 ~ Duplicate - Serial 64;
Page 142 ~ Duplicate - Serial 64;
Page 143 ~ Duplicate - Serial 64;
Page 144 ~ Duplicate - Serial 64;
Page 145 ~ Duplicate - Serial 64;
Page 146 ~ Duplicate - Serial 64;
Page 147 ~ Duplicate - Serial 64;
Page 148 ~ Duplicate - Serial 64;
Page 149 ~ Duplicate - Serial 64;
Page 150 ~ Duplicate - Serial 64;
Page 151 ~ Duplicate - Serial 64;
Page 152 ~ Duplicate - Serial 64;
Page 153 ~ Duplicate - Serial 64;
Page 154 ~ Duplicate - Serial 64;
Page 155 ~ Duplicate - Serial 64;
Page 156 ~ Duplicate - Serial 64;
Page 157 ~ Duplicate - Serial 64;
Page 158 ~ Duplicate - Serial 64;
Page 159 ~ Duplicate - Serial 64;
Page 160 ~ Duplicate - Serial 64;
Page 161 ~ Duplicate - Serial 64;
Page 162 ~ Duplicate - Serial 64;
Page 163 ~ Duplicate - Serial 64;
Page 164 ~ Duplicate - Serial 64;
Page 165 ~ Duplicate - Serial 64;
Page 166 ~ Duplicate - Serial 64;
Page 167 ~ Referral/Direct;
Page 168 ~ Duplicate - Serial 64;
Page 169 ~ Duplicate - Serial 64;
Page 170 ~ Duplicate - Serial 64;
Page 171 ~ Referral/Direct;
Page 172 ~ Referral/Direct;
Page 173 ~ Duplicate - Serial 64;
Page 174 ~ Duplicate - Serial 64;
Page 175 ~ Duplicate - Serial 64;
Page 176 ~ Duplicate - Serial 64;
Page 177 ~ Duplicate - Serial 64;
Page 178 ~ Duplicate - Serial 64;
Page 179 ~ Duplicate - Serial 64;
Page 180 ~ Duplicate - Serial 64;
Page 182 ~ Referral/Direct;

Page 183 ~ Referral/Direct;
Page 184 ~ Referral/Direct;
Page 185 ~ Referral/Direct;
Page 186 ~ Referral/Direct;
Page 187 ~ Referral/Direct;
Page 188 ~ Referral/Direct;
Page 189 ~ Referral/Direct;
Page 190 ~ Referral/Direct;
Page 191 ~ Referral/Direct;
Page 192 ~ Referral/Direct;
Page 193 ~ Referral/Direct;
Page 194 ~ Referral/Direct;
Page 195 ~ Referral/Direct;
Page 196 ~ Referral/Direct;
Page 197 ~ Referral/Direct;
Page 198 ~ Referral/Direct;
Page 199 ~ Referral/Direct;
Page 200 ~ Referral/Direct;
Page 201 ~ Referral/Direct;
Page 202 ~ Referral/Direct;
Page 203 ~ Referral/Direct;
Page 204 ~ Referral/Direct;
Page 205 ~ Referral/Direct;
Page 206 ~ Referral/Direct;
Page 207 ~ Referral/Direct;
Page 208 ~ Referral/Direct;
Page 209 ~ Referral/Direct;
Page 210 ~ Referral/Direct;
Page 211 ~ Referral/Direct;
Page 213 ~ Duplicate - Serial 65;
Page 214 ~ Duplicate - Serial 65;
Page 215 ~ Duplicate - Serial 65;
Page 217 ~ Duplicate - Serial 65;
Page 219 ~ Duplicate - Serial 66;
Page 220 ~ Duplicate - Serial 66;
Page 222 ~ Duplicate - Serial 66;
Page 225 ~ Duplicate - Serial 66;
Page 226 ~ Duplicate - Serial 66;
Page 234 ~ Duplicate - Serial 66;
Page 235 ~ Duplicate - Serial 66;
Page 236 ~ Duplicate - Serial 66;
Page 237 ~ Duplicate - Serial 66;
Page 238 ~ Duplicate - Serial 66;
Page 239 ~ Duplicate - Serial 66;
Page 240 ~ Duplicate - Serial 66;
Page 241 ~ Duplicate - Serial 66;
Page 242 ~ Duplicate - Serial 66;
Page 252 ~ Duplicate - Serial 66;
Page 253 ~ Duplicate - Serial 66;
Page 254 ~ Duplicate - Serial 66;
Page 255 ~ Duplicate - Serial 66;
Page 256 ~ Duplicate - Serial 66;
Page 257 ~ Duplicate - Serial 66;
Page 258 ~ Duplicate - Serial 66;
Page 259 ~ Duplicate - Serial 66;
Page 260 ~ Duplicate - Serial 17;
Page 263 ~ Duplicate - Serial 17;
Page 266 ~ Duplicate - Serial 66;
Page 272 ~ Duplicate - Serial 66;
Page 279 ~ Duplicate - Serial 61;
Page 280 ~ Duplicate - Serial 61;
Page 281 ~ Duplicate - Serial 61;
Page 282 ~ Duplicate - Serial 61;
Page 283 ~ Duplicate - Serial 61;

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

139

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-18-2012 BY [redacted]

~~Secret~~

FBI IORC Representatives' Log

Updated 02/12/98 3:13 AM

11 February 1998

12:00a Received a faxed copy of requested Internet searches on ISP data from [redacted] @ the CITAC Watch desk. b6 b7C

There was no material available on current FBI operations, plans, programs, or courses of action. There was no information available on FBI liaison activities with other Federal agencies.

2:00a [redacted]

3:00a [redacted] Referral/Consult

3:45a MSH delivered site summary and LEA update slides to [redacted] for inclusion into the morning briefing.

4:00a MSH faxed the 10 FEB 98 FBI IORC Rep's log to the CITAC Watch desk.

4:30a [redacted]

5:30a [redacted]

288-HQ-1242560

w: citac
from: IORC

Record # 40
logged 2/12/98 [redacted] b6 b7C

288 HQ-1345 30-61

~~Secret~~

2/12/98 AM

~~Secret~~

FBI IORC Representatives' Log

Updated 02/12/98 3:13 AM

6:30 CFS assumes watch duty. MSH briefs CFS to action items.

6:31 [redacted]

Info from CSIS standup. Referral/Consult

- Waiting on CITAC Watch daily summary.

[redacted]

8:30 Passed hot list to [redacted] Items included: b6 b7C

(1) Conduct ACS search on [redacted] b6 b7C

(2) Conduct Newsgroup search on [redacted]

(3) Status of the UNC site. Was it served? What did we get?

[redacted]

Updated items: Referral/Consult

[redacted]

9:00 Spoke with [redacted] CIU, CITAC-Working with CERT to confirm any similar (IMAP, PHF, RPC) exploits on civilian side. b6 b7C

9:30 [redacted] Referral/Consult

[redacted]

10:00

10:45 CITAC Watch search of ACS: No hits on [redacted] b6 b7C

[redacted] Referral/Consult

~~Secret~~

~~Secret~~

FBI IORC Representatives' Log

Updated 02/12/98 3:13 AM

- 2703D served at [redacted] b3 b7E
- UNC subpoena has NOT been served.

[redacted]

11:30 [redacted] Referral/Consult
-2703D have been served on all previously identified sites including [redacted] b3 b7E
-FBI will serve warrants on all .edu sites.
By approximately 14:00 today warrant will be served on Maroon.com

12:00 Prepare bullets for FBI presentation to DEPSECDEF at 1530.

1:00 CFS departs IORC, Pentagon for FBIHQ

5:00 CFS returns to IORC

6:45p CFS briefs MSH on current situation. Three issues are outstanding:

- There are problems with sharing law-enforcement sensitive information with the entire J39 cell and interagency liaison community. (At the last minute, the LEA briefing slide for the 3:30p briefing was pulled as a result of these sensitivities.) b6
- Ken Geide and [redacted] attended the 3:30p briefing with [redacted] b7C [redacted] reporting that LEA activities were underway, but that details of investigations could not be divulged. Referral/Consult
- Shift changes may be imminent as a result of manpower stresses at FBI HQ and a reduced need for a person at the IORC based on changes in FBI - IORC information exchange procedures. Decisions on this will be taken at CITAC HQ.

7:00p MSH assumes station, and listens in on the latter part of the change-of-station briefing.

7:30p MSH has an off-line conversation with [redacted]

[redacted]

- The FBI liaison schedule will be reconsidered. Referral/Consult

7:50p MSH calls CITAC HQ and speaks with Ken Geide. MSH authorizes the individual briefing to [redacted] The issue of support to this briefing and to other briefings is also discussed. Mr. Geide said that [redacted] should feel free to call him with any outstanding questions.

~~Secret~~

FBI IORC Representatives' Log

Updated 02/12/98 3:13 AM

Mr. Geide suggests that two regularly scheduled updates can be sent to the FBI IORC rep to be included in this briefing, though this may not occur tonight.

Referral/Consult

8:00p [redacted]

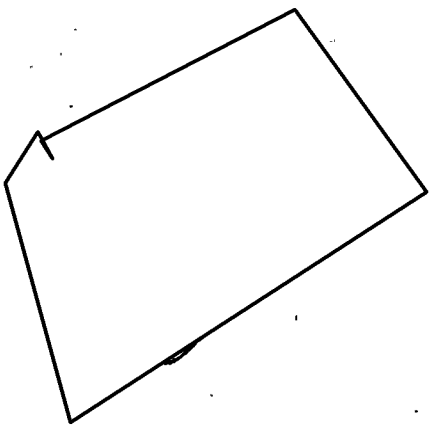
8:20p Both [redacted]

9:29p Received faxed copy of day's FBI case activity from [redacted] b6 b7C

9:45p JSAN user id and password given to FBI reps.

11:55p [redacted]

Referral/Consult



b6
b7C

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-25-2012 BY [redacted]

429

Daily Report of Leads Completed

2/13/98 3:57:10 PM

Received On: 2/11/98 **Source Document:** E-Mail

Detail Date: 2/11/98 **Detail Time:**

Subject: IRC Monitoring

Lead Received From: IOS [redacted] b6 b7C

Lead Assigned To: **Lead Due On:**

Referral/Consult

Details:

[redacted]

288 - HQ - 1245760

from:

to:

[redacted] b6 b7C

288-HQ-1345760-65

Received On: 2/2/98 **Source Document:** Other

Detail Date: 2/2/98 **Detail Time:** 1:35:00 PM

Subject: [redacted]

Lead Received From: SSA [redacted]

Lead Assigned To: [redacted] **Lead Due On:**

b6
b7C
b7E

Details: Floppy disc received from [redacted] with a listing of [redacted] can be reached on Ext. [redacted]

Received On: 2/9/98 **Source Document:** EC

Detail Date: 2/9/98 **Detail Time:**

Subject: Unsub(s); Multiple Intrusions into DOD Facilities

Lead Received From: SSA [redacted]

Lead Assigned To: [redacted] **Lead Due On:** 2/9/98 b6 b7C

Details: The above-EC was drafted by [redacted] requesting the opening of a Headquarters case.

On this same date, IOS [redacted] contacted [redacted] Division 4, who established the following file number for this case: 288-HQ-1242560

Received On: 2/10/98 **Source Document:** Phone Message

Detail Date: 2/10/98 **Detail Time:**

Subject: CERT

Lead Received From: SSA [redacted]

Lead Assigned To: IOS [redacted] **Lead Due On:**

b6
b7C

Details: [redacted] is to send her information

Received On: 2/10/98 **Source Document:** EC

Detail Date: 2/10/98 **Detail Time:**

Subject: Unsubs; Multiple Intrusions into DOD Facilities

Lead Received From: SSA [redacted]

Lead Assigned To: Laboratory/WFO **Lead Due On:** 2/11/98

Details: COORDINATED BY SSA [redacted]

b6
b7C

CART at HQ and WFO is requested to determine the proper location & procedure to conduct the CART duplication & examinations on an expedited basis, & advise CITAC of its decision by COB 2/11/98. It is also requested that approximate CART processing time be provided.

A copy of this lead was facsimiled to WFO. A copy of this lead was also hand carried to CART.

SSA [redacted] advised that , per SSA [redacted] CART, WFO should handle the matter. This matter was resolved on 2/11/98

Received On:	2/12/98	**Source Document:**	E-Mail
Detail Date:	2/12/98	**Detail Time:**	10:29:00 AM

Subject: Computer Viruses

Lead Received From: IOS [redacted] b6 b7C

Lead Assigned To: Watch **Lead Due On:**

Details: Report any significant history of computer viruses for the month of February.

As of 2/12/98 - IOS [redacted] this lead was covered by the watch and a copy of the information that was sent to [redacted] will be given to [redacted] b6 b7C Referral/Consult

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-18-2012 BY [redacted]

4/39

Daily Report of Pending Leads

2/13/98 3:57:05 PM

Lead Assigned To:

Lead Received From: IOS [redacted] b6 b7C

Received On: 2/11/98

Source Document: E-Mail

Detail Date: 2/11/98

Detail Time:

Subject: IRC Monitoring

Referral/Consult

Details: [redacted]

288-HQ-1242560

[redacted] b6 b7C

Serial 1

288-HQ-1242560-66

Lead Assigned To:

Lead Received From:

Received On: 2/11/98

Source Document: E-Mail

Detail Date: 2/11/98

Detail Time:

Subject: IRC Monitoring

Referral/Consult

Details:

Lead Assigned To:

Lead Received From: IOS [redacted] b6 b7C

Received On: 2/11/98

Source Document: E-Mail

Detail Date: 2/11/98

Detail Time:

Subject: IRC Monitoring

Referral/Consult

Details: [redacted]

Lead Assigned To:

Lead Received From: IOS [redacted] b6 b7C

Received On: 2/11/98

Source Document: E-Mail

Detail Date: 2/11/98

Detail Time:

Subject: IRC Monitoring Referral/Consult

Details: [redacted]

Lead Assigned To: All Entities

Lead Received From: SSA [redacted] b6 b7C

Received On: 2/11/98

Source Document: Write-Up

Detail Date: 2/11/98

Detail Time:

Subject: Indices Checks

Details: Conduct appropriate indices checks - statd, etc.

Lead Assigned To: [redacted]

Lead Received From: SSA [redacted]

b6
b7C

Received On: 2/11/98

Source Document: Write-Up

Detail Date: 2/11/98

Detail Time:

Subject: 2703 (d)

Details: Obtain 2703(d) response.

Lead Assigned To: [redacted]

Lead Received From: SSA [redacted]

b6
b7C

Received On: 2/12/98

Source Document: Write-Up

Detail Date: 2/12/98

Detail Time: 10:00:00 AM

Subject: Navy Case

Details: Get update on Navy case in Florida.

Lead Assigned To: IOS [redacted]

Lead Received From: SSA [redacted]

Received On: 2/10/98

Source Document: Voice Message

Detail Date: 2/10/98

Detail Time:

b6
b7C

Subject: CERT

Details: [redacted] is to set up a meeting between himself and [redacted] to discuss information passed on to CERT.

Lead Assigned To:	Legat Israel	**Lead Received From:**	SSA [redacted] b6 b7C
Received On:	2/11/98	**Source Document:**	Write-Up
Detail Date:	2/11/98	**Detail Time:**	

Subject: Parliment Website

Details: Lead to Legat Israel Re: Penetration of Parliment Web-Site

Lead Assigned To: [redacted] San Franc **Lead Received From:** SSA [redacted] b6 b7C

Received On: 2/12/98 **Source Document:** Write-Up

Detail Date: 2/12/98 **Detail Time:** 10:00:00 AM

Subject: University of Maryland

Details: Tagging of hacker tools at the University of Maryland

Lead Assigned To: [redacted] WFO

Lead Received From: SSA [redacted]

b6
b7C

Received On: 2/11/98

Source Document: Write-Up

Detail Date: 2/11/98

Detail Time:

Subject: Trap and Trace Order

Details: [redacted]

b3

Lead Assigned To: SSA [redacted]

Lead Received From: SSA [redacted]

b6
b7C

Received On: 2/12/98

Source Document: Write-Up

Detail Date: 2/12/98

Detail Time: 10:00:00 AM

Subject: Profile Requests

Details: Draft response to profile requests.

Lead Assigned To: SSA [redacted]

Lead Received From: SSA [redacted]

b6
b7C

Received On: 2/12/98

Source Document: Write-Up

Detail Date: 2/12/98

Detail Time: 10:00:00 AM

Subject: Gospelcom.net

Details: Gospelcom.net

Lead Assigned To: SSA [redacted]

Lead Received From: SSA [redacted]

b6
b7C

Received On: 2/12/98

Source Document: Write-Up

Detail Date: 2/12/98

Detail Time: 10:00:00 AM

Subject: Lead to all field offices

Details: Lead to all field offices: check all logical sources

Lead Assigned To: SSA [redacted]

Lead Received From: SSA [redacted]

b6
b7C

Received On: 2/11/98

Source Document: Write-Up

Detail Date: 2/11/98

Detail Time:

Subject: Gospelcom.Net

Details: Coordinate Gospelcom.net investigation.

Lead Assigned To: SSA [redacted]

Lead Received From: SSA [redacted]

Received On: 2/12/98

Source Document: Write-Up

Detail Date: 2/12/98

Detail Time: 10:00:00 AM

b6
b7C

Subject: [redacted]

Details: Pursue [redacted] case.

Lead Assigned To: SSA [redacted]

Lead Received From: SSA [redacted]

b6
b7C

Received On: 2/11/98

Source Document: Write-Up

Detail Date: 2/11/98

Detail Time:

Subject: Request for Information

Details: [redacted] Referral/Consult

Lead Assigned To: SSA [redacted]

Lead Received From: SSA [redacted] b6 b7C

Received On: 2/11/98

Source Document: Write-Up

Detail Date: 2/11/98

Detail Time:

Subject:

Details: EC to WFO: Open separate Navy case [redacted] Referral/Consult

Lead Assigned To:	SSA [redacted]	**Lead Received From:**	SSA [redacted]
Received On:	2/11/98	**Source Document:**	Write-Up
Detail Date:	2/11/98	**Detail Time:**	2:55:00 PM
Subject:	Facsimile		

b6
b7C

Details: Fax All Field Office EC and list of sites hit to Cleveland Attn: [redacted]

~~28~~

Lead Assigned To: SSA [redacted]

Lead Received From: SSA [redacted]

b6
b7C

Received On: 2/11/98

Source Document: Write-Up

Detail Date: 2/11/98

Detail Time:

Subject: Hacker Case

Details: Get details about Cleveland hacker case.

Lead Assigned To: SSA [redacted]

Lead Received From:

b6
b7C

Received On: 2/11/98

Source Document: Write-Up

Detail Date: 2/11/98

Detail Time:

Subject: TR #

Details: Obtain TR #

30

Lead Assigned To:	WFO	**Lead Received From:**	SSA [redacted]
Received On:	2/12/98	**Source Document:**	Write-Up
Detail Date:	2/12/98	**Detail Time:**	10:00:00 AM

b6
b7C

Subject: Interviews

Details: Interview sys-admin at University of Maryland re: hacker tool files

~~31~~

Lead Assigned To:	WFO at Falls Church,	**Lead Received From:**	SSA [redacted] b6 b7C
Received On:	2/12/98	**Source Document:**	EC
Detail Date:	2/12/98	**Detail Time:**	2:12:00 PM

Subject: Unknown Subjects;
Multiple Intrusions into DOD Facilities (288-HQ-1242560-18)

Details: Prepare for evidence storing and CART processing. Upon receipt of materials prepare two copies of each, [redacted] Referral/Consult

~~32~~

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-19-2012 BY [redacted]

439

from: [redacted]
to:

b6
b7C

Leads: 2/16/98 5:00PM

SF:

Will obtaan [redacted]

Will begin surviellance of [redacted]

Will obtain revised trap and trace for [redacted]

Will continue T-III monitoring of [redacted]

Will continue Pen register on [redacted]

Will execute trap and trace for subject #2.

Will conduct logical investigation of [redacted]

Will amend T-III order to obtain [redacted]

288-HQ-1242560

b3
b7E

Hoston:

WFO:

Will contact and interview [redacted] Obtain all relevant records.

b3

[redacted] / Gospelnet.com investigation.

[redacted] investigation : EAPNET/CLARKNET.

b6
b7C

Followup with University of Maryland.

[redacted]

Referral/Consult

Boston:

288-HQ-1242560-67

[redacted]

Will Seek consent search from Sys Admin and all users.

FBIHQ:

✓ Followup on efforts at Utah State, Notre Dame, University of Conn.

✓ Will conduct checks of indices and publice records for all entities.

✓ [redacted] Referral/Consult

✓ Check significant of "ll" and 3/26/97.

✓ Check UNC logs for other victim sites. Run indices checks on all lsited sites.

✓ Obtain orders for tagging of University of Maryland tools.

✓ Open FCI case (297 to be opened)

Draft response to profile requests [redacted] b6 b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-19-2012 BY [redacted]

Automated Serial Permanent Charge-Out
FD-5a (1-5-94)

Date: 02/17/98 Time: 12:48

Case ID: 288-HQ-1242560 Serial: 68

Description of Document:

Type : FAX
Date : 02/10/98
To : CITAC
From : [redacted]
Topic: UPDATE ON ACTIVITIES

Reason for Permanent Charge-Out: b6 b7C

SHOULD NOT HAVE SERIALIZED

Employee: [redacted]

(12/31/1995)

DECLASSIFIED BY [redacted]
ON 09-19-2012

429

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 02/17/1998

To: Houston **Attn:** [redacted]
(CITA Supervisor)

San Francisco **Attn** [redacted]
(CITA Supervisor)

Washington Field Office **Attn:** [redacted]
(CITA Supervisor)

b6
b7C

From: NSD/CID
OCCIP/CITAC/Room 11887
Contact: IOS [redacted]

Approved By: Geide Kenneth M [redacted]

b6
b7C

Drafted By: [redacted] :apm

Case ID #: (U) ~~(S)~~ 288-HQ-1242560-69 (Pending)

Title: (U) ~~(S)~~ SOLAR SUNRISE;
CITAC MATTERS;
OO: HQ;

Synopsis: (U) ~~(S)~~ Request for status report on DOD intrusions.

(U) ~~(S)~~ ~~**Classified By: 4511, CITAC/NSD**~~
~~**Reason : 1.5(c)**~~
~~**Declassify On: 02/12/2008**~~

Details: (U) ~~(S)~~ Due to the increasing demand for updates and briefings to DOD, the AG, and other government agencies regarding the intrusions into Department of Defense's (DOD) computer systems, each CITA team is to report a daily status to CITAC on this investigation by 7:00p.m.(EST). This status report can be faxed to the attention, Kenneth Geide, or [redacted] CITAC, fax number [redacted] (unsecure), [redacted] (secure).

b6
b7C

~~SECRET~~

To: Houston From: NSD/CID
Re: (U) ~~(S)~~ 288-HQ-1242560, 02/17/1998

LEAD (s):

Set Lead 1:

ALL RECEIVING OFFICES

All offices are to report case status daily to CITAC, attention Kenneth Geide.

CC: 1 - Mr. Geide
1 - [redacted]
1 - [redacted]
1 - [redacted]
1 - [redacted]

b6
b7C

♦♦

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-19-2012 BY [redacted]

439

2/10/98

To: [redacted]

b6
b7C

From: [redacted] IT-Middle East Unit -
NS-3B, Ext. [redacted]

[redacted]

b7E

has bulky Enclosure

288-HQ-1242560-72

288-HQ-1242560

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-25-2012 BY [redacted]

434

Daily Report of Leads Completed

2/18/98 8:13:37 AM

Received On: 2/11/98 **Source Document:** E-Mail

Detail Date: 2/11/98 **Detail Time:**

Subject: IRC Monitoring

Lead Received From: IOS [redacted] b6 b7C

Lead Assigned To: **Lead Due On:**

Referral/Consult

Details: [redacted]

from: [redacted] b6 b7C

to

288-HQ-1345[illegible]-78

Received On: 2/10/98 **Source Document:** EC

Detail Date: 2/10/98 **Detail Time:**

Subject: Unsubs; Multiple Intrusions into DOD Facilities

Lead Received From: SSA [redacted]

Lead Assigned To: Laboratory/WFO **Lead Due On:** 2/11/98

b6
b7C

Details: COORDINATED BY SSA [redacted]

CART at HQ and WFO is requested to determine the proper location & procedure to conduct the CART duplication & examinations on an expedited basis, & advise CITAC of its decision by COB 2/11/98. It is also requested that approximate CART processing time be provided.

A copy of this lead was facsimiled to WFO. A copy of this lead was also hand carried to CART.

SSA [redacted] advised that , per SSA [redacted] CART, WFO should handle the matter. This matter was resolved on 2/11/98.

b6
b7C

On 2/17/98 the [redacted]

b7E

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-19-2012 BY [redacted]

439

Daily Report of Pending Leads

2/18/98 8:13:32 AM

Lead Assigned To:

Lead Received From: IOS [redacted] b6 b7C

Received On: 2/11/98

Source Document: E-Mail

Detail Date: 2/11/98

Detail Time:

Subject: IRC Monitoring

Referral/Consult

Details: [redacted]

from: [redacted] b6 b7C

to:

[redacted]

[redacted]

[redacted]

Lead Assigned To:

Lead Received From: IOS [redacted] b6 b7C

Received On: 2/11/98

Source Document: E-Mail

Detail Date: 2/11/98

Detail Time:

Subject: IRC Monitoring

Referral/Consult

Details: [redacted]

Lead Assigned To:	Boston	**Lead Received From:**	SSA [redacted] b6 b7C
Received On:	2/17/98	**Source Document:**	Write-Up
Detail Date:	2/16/98	**Detail Time:**	5:00:00 PM

Subject:

Details: Seek consent search from Sys Admin and all users.

Lead Assigned To:	Boston	**Lead Received From:**	SSA [redacted] b6 b7C
Received On:	2/17/98	**Source Document:**	Write-Up
Detail Date:	2/16/98	**Detail Time:**	5:00:00 PM
Subject:			Referral/Consult
Details:	[redacted]		

Lead Assigned To:	FBIHQ	**Lead Received From:**	SSA [redacted]
Received On:	2/17/98	**Source Document:**	Write-Up
Detail Date:	2/16/98	**Detail Time:**	5:00:00 PM

b6
b7C

Subject:

Details: Will conduct checks of indices and public records for all entities.

Lead Assigned To:	FBIHQ	**Lead Received From:**	SSA [redacted]
Received On:	2/17/98	**Source Document:**	Write-Up
Detail Date:	2/16/98	**Detail Time:**	5:00:00 PM

b6
b7C

Subject:

Details: Follow-up on efforts at Utah State, Notre Dame, University of Conn.

Lead Assigned To:	FBIHQ	**Lead Received From:**	SSA [redacted] b6 b7C
Received On:	2/17/98	**Source Document:**	Write-Up
Detail Date:	2/16/98	**Detail Time:**	5:00:00 PM

Subject:

Details: [redacted] Referral/Consult

Lead Assigned To:	FBIHQ	**Lead Received From:**	SSA [redacted] b6 b7C
Received On:	2/17/98	**Source Document:**	Write-Up
Detail Date:	2/16/98	**Detail Time:**	5:00:00 PM

Subject:

Details: [redacted] Referral/Consult

Lead Assigned To:	FBIHQ	**Lead Received From:**	SSA [redacted]
Received On:	2/17/98	**Source Document:**	Write-Up
Detail Date:	2/16/98	**Detail Time:**	5:00:00 PM

b6
b7C

Subject:

Details: Check UNC logs for other victim sites. Run indices checks on all listed sites.

Lead Assigned To:	FBIHQ	**Lead Received From:**	SSA [redacted]
Received On:	2/17/98	**Source Document:**	Write-Up
Detail Date:	2/16/98	**Detail Time:**	5:00:00 PM

b6
b7C

Subject:

Details: Obtain orders for tagging of University of Maryland tools.

Lead Assigned To: FBIHQ

Lead Received From: SSA [redacted] b6 b7C

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

Subject:

Details: Open FCI case (297 to be opened)

Lead Assigned To: San Francisco

Lead Received From: SSA [redacted] b6 b7C

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

Subject:

Details: Continue Pen Register on [redacted] b3

Lead Assigned To:	San Francisco	**Lead Received From:**	SSA [redacted] b6 b7C
Received On:	2/17/98	**Source Document:**	Write-Up
Detail Date:	2/16/98	**Detail Time:**	5:00:00 PM
Subject:	288-HQ-1242560		

Details: Obtain [redacted] b3

Lead Assigned To:	San Francisco	**Lead Received From:**	SSA [redacted]	b6 b7C
Received On:	2/17/98	**Source Document:**	Write-Up	
Detail Date:	2/16/98	**Detail Time:**	5:00:00 PM	

Subject:

Details: Begin surveillance of [redacted] b3

Lead Assigned To:	San Francisco	**Lead Received From:**	SSA [redacted] b6 b7C
Received On:	2/17/98	**Source Document:**	Write-Up
Detail Date:	2/16/98	**Detail Time:**	5:00:00 PM

Subject:

Details: Continue T-III monitoring of [redacted] b3

Lead Assigned To:	San Francisco	**Lead Received From:**	SSA [redacted]
Received On:	2/17/98	**Source Document:**	Write-Up
Detail Date:	2/16/98	**Detail Time:**	5:00:00 PM

b6
b7C

Subject:

Details: Execute Trap and Trace for subject #2

Lead Assigned To:	San Francisco	**Lead Received From:**	SSA [redacted] b6 b7C
Received On:	2/17/98	**Source Document:**	Write-Up
Detail Date:	2/16/98	**Detail Time:**	5:00:00 PM

Subject:

Details: Conduct logical investigation of [redacted] b7E

Lead Assigned To:	San Francisco	**Lead Received From:**	SSA [redacted]	b6 b7C
Received On:	2/17/98	**Source Document:**	Write-Up	
Detail Date:	2/16/98	**Detail Time:**	5:00:00 PM	

Subject:

Details: Amend T-III order to obtain [redacted] b3

Lead Assigned To:	San Francisco	**Lead Received From:**	SSA [redacted] b6 b7C
Received On:	2/17/98	**Source Document:**	Write-Up
Detail Date:	2/16/98	**Detail Time:**	5:00:00 PM

Subject:

Details: Obtain revised trap and trace for [redacted] b3

Lead Assigned To: SSA [redacted]

Lead Received From: SSA [redacted]

b6
b7C

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

Subject:

Details: Draft response to profile requests.

Lead Assigned To: SSA [redacted]

Lead Received From: SSA [redacted]

b6
b7C

Received On: 2/11/98

Source Document: Write-Up

Detail Date: 2/11/98

Detail Time:

Subject:

Details: Open FCI Case

Lead Assigned To: SSA [redacted] **Lead Received From:** SSA [redacted] b6 b7C

Received On: 2/11/98 **Source Document:** Write-Up

Detail Date: 2/11/98 **Detail Time:**

Subject: Harvard

Details: Follow up with Boston on service to Harvard

Lead Assigned To: SSA [redacted]

Lead Received From: SSA [redacted]

b6
b7C

Received On: 2/11/98

Source Document: Write-Up

Detail Date: 2/11/98

Detail Time:

Subject: Hacker Case

Details: Get details about Cleveland hacker case.

Lead Assigned To: SSA [redacted]

Lead Received From: b6 b7C

Received On: 2/11/98

Source Document: Write-Up

Detail Date: 2/11/98

Detail Time:

Subject: TR #

Details: Obtain TR #

Lead Assigned To:	WFO	**Lead Received From:**	SSA [redacted]	b6 b7C
Received On:	2/17/98	**Source Document:**	Write-Up	
Detail Date:	2/16/98	**Detail Time:**	5:00:00 PM	

Subject:

Details: Contact and interview [redacted] Obtain all relevant records. b3

Lead Assigned To:	WFO	**Lead Received From:**	SSA [redacted]
Received On:	2/17/98	**Source Document:**	Write-Up
Detail Date:	2/16/98	**Detail Time:**	5:00:00 PM

b6
b7C

Subject:

Details: [redacted] Gospelnet.com investigation

Lead Assigned To: WFO

Lead Received From: SSA [redacted]

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

b6
b7C

Subject:

Details: [redacted] investigation:EAPNET/CLARKNET

Lead Assigned To: WFO

Lead Received From: SSA [redacted] b6 b7C

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

Subject:

Details: Follow-up with University of Maryland

Lead Assigned To: WFO

Lead Received From: SSA [redacted] b6 b7C

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

Subject: Referral/Consult

Details: Contact [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-19-2012 BY [redacted]

439

From: [redacted] b6
To: [redacted] b7C
Date: February 18, 1998 (Wednesday) 8:05 am
Subject: LEADS [redacted] -Reply

[redacted] b7E

288-HQ-1042560

288-HQ-1042560-80

(12/31/1995)

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-19-2012 BY [redacted]

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 02/18/1998

To: Boston Attn: SSA [redacted]
Houston Attn: SSA
San Francisco Attn: SSA
WMFO Attn: SSA

From: NSD/CID/CITAC
Contact: SSA [redacted]

b6
b7C

Approved By: Geide Ken M

Drafted By: [redacted] :hg

Case ID #: 288-~~HQ~~-1242560-~~8~~ (Pending)

Title: OPERATION SOLAR SUNRISE
CITA MATTERS
OO:HQ

Synopsis: This communication sets forth additional investigative leads to be addressed regarding captioned subject.

(U) ~~(S)~~

~~**Classified By: 4511, CITAC/D5**~~
~~**Reason : 1.5(c)**~~
~~**Declassify On: x-1**~~

Administrative: Receiving field offices should reference Bureau EC to All Field Offices, dated 2/9/98; Bureau EC to All Field Offices dated 2/12/98.

Referral/Consult

Details: (S) Referenced matter continues to receive the highest level of attention and scrutiny from the Department of Defense and the National Security Council. The Attorney General has ordered all necessary DOJ resources be afforded to this matter, and all avenues of investigation be pursued. FBIHQ will continue to provide overall coordination, analytical support and liaison with DOD, [redacted] under umbrella case 288-HQ-1242560. The following leads delineate specific areas of investigative responsibility for receiving field offices, under which field office of origin (OO) cases may be opened. Investigation and leads should be expeditiously addressed and telephonically provided to

~~SECRET~~

To: Boston From: NSD/CID/CITAC
Re: 288-NQ-1242560, 02/18/1998

SSA [redacted] or Acting Unit Chief [redacted] These telephonic contacts should be followed up with appropriate paper communications. b6 b7C

To: Boston From: NSD/CID/CITAC
Re: 288-NQ-1242560, 02/18/1998

LEAD (s):

Set Lead 1:

BOSTON

AT BOSTON, MA

Referral/Consult

Set Lead 2:

HOUSTON

Referral/Consult

AT HOUSTON, TX

(U) ~~X~~

Set Lead 3:

SAN FRANCISCO

AT SAN FRANCISCO, CA

(U) ~~(S)~~ Will open an OO case into intrusions in to department of defense domain name servers and b7E

(U) ~~(S)~~ Will continue T-III monitoring of perform analysis of content and provide results to CITAC. Will obtain b3 and conduct appropriate analysis.

(U) (S) Will initiate surveillance of subjects, as deemed appropriate.

(U) (S) Will seek amended T-III order or letter from [redacted] b3

(U) (S) Will consider use of [redacted] b6 b7C b7E

Set Lead 4:

WMFO

AT WASHINGTON, DC

(U) (S) Will contact and interview [redacted] regarding trace of Internet session accessed through [redacted] Obtain all relevant records. b3

[redacted] Referral/Consult

(U) (S) Will continue investigation into [redacted] and coordinate with NCIS. b6 b7C

(U) (S) Will obtain and serve 2703 D order on University of Maryland systems administrator to determine source of hacker tool files. Conduct appropriate investigation to determine user account holding and accessing files, date files were accessed and locations to which they were transferred. Will obtain trap and trace order for [redacted] b3

[redacted] Referral/Consult

CC: 1 - Mr. Geide
1 - [redacted] b6 b7C

To: Boston From: NSD/CID/CITAC
Re: 288-NQ-1242560, 02/18/1998

1 - Mr. [redacted] b6
1 - Mr. [redacted] b7C

♦♦

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-19-2012 BY [redacted]

(12/31/1995)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIROITY **Date:** 02/16/1998

To: FBI Headquarters **Attn:** CITAC
Unit Chief
[redacted] b6 b7C

From: Houston
WC-4
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted] : sfr

Case ID #: [redacted] (Pending)

Title: COMPUTER INTRUSIONS

Synopsis: Measures taken to date, measures to be taken and request of CITAC. b3 b7E

Reference: [redacted]

Details: **MEASURES TAKEN TO DATE:**

On February 9, 1998, an immediate teletype from FBIHQ was received by the Houston Division, via secure fax explaining the details of an extensive hacker investigation that linked back to a company in College Station, Texas, known as Maroon.com. [redacted]

[redacted]

[redacted] provided Agents of [redacted] Referral/Consult

[redacted]

In reviewing the [redacted] Agents found that the [redacted] contained information that was beyond the scope of the 2703(d) court order. Due to this fact, the [redacted] pending the issuance of a search warrant. b3 b7E

288-HQ-1245200

288-HQ-[redacted]-84

entered 2/19/98 [redacted]

log #65

b6 b7C

To: FBI Headquarters From: Houston
Re: [redacted] 02/16/1998

On February 14, 1998, a search warrant application was filed and a search warrant allowing the FBI total access to all data backed up from [redacted] system was signed by Judge Stacy. The back up tapes were then recovered from [redacted] by Agents of the FBI and a chain of custody was started.

On February 15, 1998, CART agent [redacted] took possession of the above referenced back up tapes and started an analysis of the data. Currently, these back up tapes are being reviewed for leads by Houston's CART trained Agents. b6 b7C b7E

Questions regarding this matter should be addressed to SA [redacted]

MEASURES TO BE TAKEN:

On February 15, 1998, a meeting of the Houston CITAC team, consisting of the following persons:

ASAC
ASAC [redacted]
SSA
SSA
SSA [redacted] b6 b7C
ASSA [redacted]
SA
SA
SA
SA
SA
SA
SA [redacted] (Answer Coordinator)
Mr. [redacted]

The purpose of the meeting was to formulate a logical process in which to cover all leads generated during this case. As a result of the meeting, the following measures will be taken:

1. Houston will immediately start Rapid Start.
2. Effective February 17, 1998, information obtained from the analysis by Special Agent [redacted] will be loaded into a rapid start. b6 b7C
3. Copies of the back up tapes obtained from Maroon.com will be forwarded to CITAC and the FBIHQ laboratory for analysis.
4. Houston Division will obtain GROUPWISE E-mail with direct access to CITAC, Strategic Information Operation Center(SIOC) and the San Francisco Division.

To: FBI Headquarters From: Houston
Re: [redacted] 02/16/1998 b7E

REQUESTS OF CITAC:

The Houston Division requests authority to obtain a STU-III (secure telephone) and a secure fax to disseminate and receive secure information generated throughout this investigation.

♦♦